

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Overview

Plaintiff accuses Defendant of infringement through making, using, selling, offering for sale, and importation of Zoho's ("Defendant" or "Zoho") ManageEngine, including Endpoint Central and Vulnerability Manager Plus (the "Accused System and Method"), and all substantially similar products. The term "Accused System and Method" includes the associated computer hardware, interfaces, software, and data, and the processes and methods related thereto.

The Accused System and Method is accused of directly infringing U.S. Patent No. 10,154,055 (the "'055 Patent"). Plaintiff further accuses Defendant of indirectly infringing the '055 Patent by providing its customers and others the Accused System and Method to utilize in an infringing manner. Defendant intends to cause infringement by its customers and users as Defendant instructs users to use the Accused System and Method in an infringing manner. Defendant deploys client software to implement the Accused System and Method. Defendant also provides support and implementation services for the Accused System and Method, including providing instructions, guides, online materials, and technical support.

The asserted claims include elements that are implemented, at least in part, by proprietary electronics and software in the Accused System and Method. The precise designs, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of Defendant's documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused System and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff. Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of the Court's final claim construction in this action and in connection with the provision of its expert reports.

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

10,154,055 Claim 7	Evidence
<p>An apparatus, comprising: at least one platform; an intrusion prevention system component that is communicatively coupled with the at least one platform;</p>	<p>ManageEngine includes <i>at least one platform</i> (e.g., ManageEngine serving as a platform); <i>an intrusion prevention system</i> (e.g., The vulnerability information collected across multiple endpoints which also includes antivirus option) <i>component that is communicatively coupled with the at least one platform</i> (e.g., Manage Engine serving as a platform for the vulnerability manager plus and firewall);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Enterprise vulnerability management software

Vulnerability Manager Plus is a multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions. Learn how to perform step-by-step [vulnerability management](#) in your enterprise with Vulnerability Manager Plus.

Scan



Scan and discover exposed areas of all your local and remote office endpoints as well as roaming devices.

Assess



Leverage attacker-based analytics, and prioritize areas that are more likely to be exploited by an attacker.

Manage



Mitigate the exploitation of security loopholes that exist in your network and prevent further loopholes from developing.

<https://www.manageengine.com/vulnerability-management/?pos=EndpointCentral&loc=ProdMenu&cat=UEMS>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Comprehensive vulnerability scanning

Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:

- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.

<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus dashboard. The left sidebar lists various threat categories, with 'Zero-day Vulnerabilities' highlighted. The main panel displays a table of zero-day vulnerabilities. The table has columns for 'Threats', 'Threat Category', 'Affected Systems', and 'Action'. The data rows include Google Chrome (x64) (78.0.3904.87), 2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20..., and 2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200... Each row shows a 'Fix' button. The interface also includes a search bar, a filter dropdown, and a 'Total: 5' indicator.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_6_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

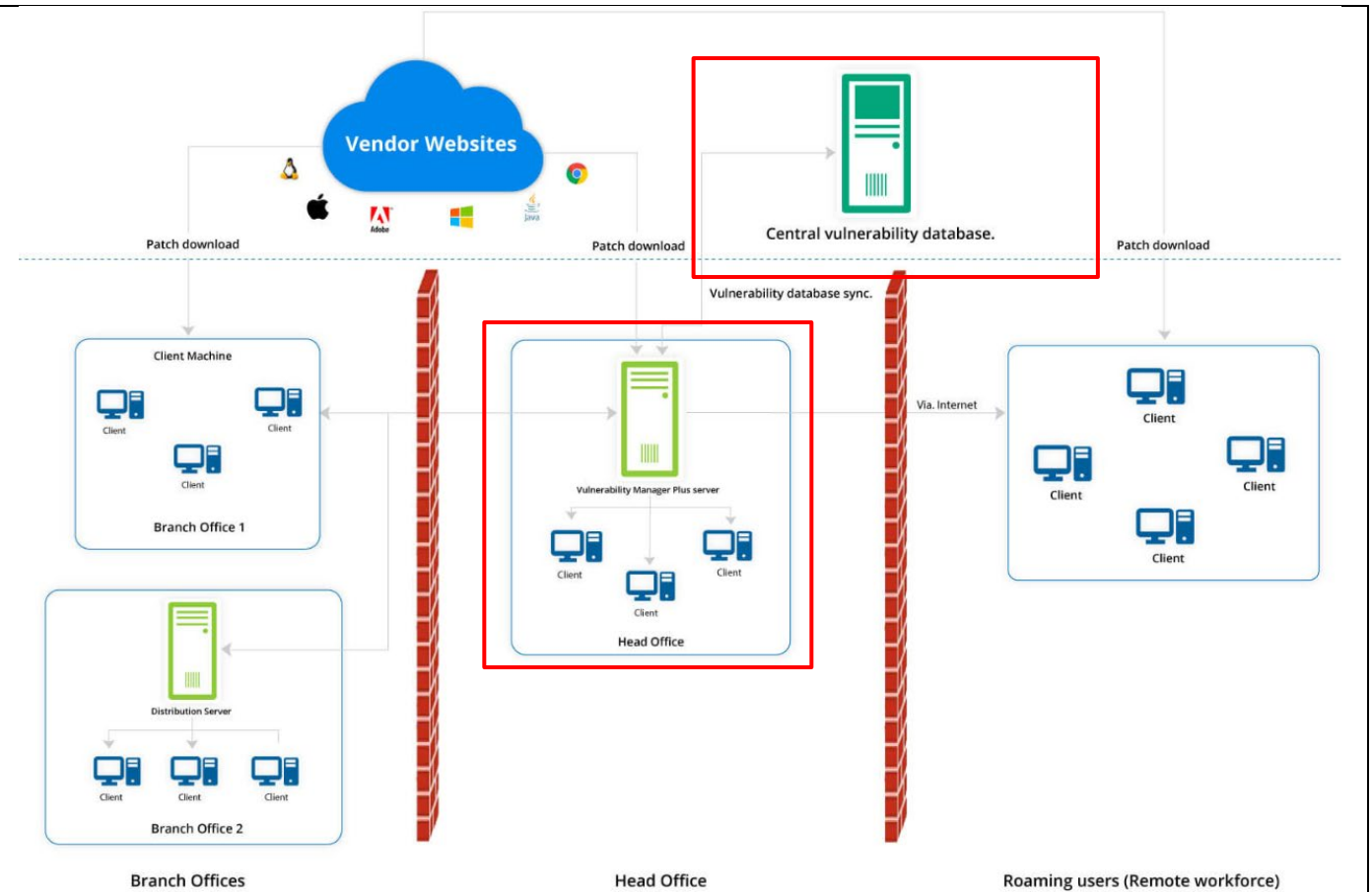
Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of

privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

<https://www.manageengine.com/security.html?mesearch>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary

Zero-day
vulnerabilities

Vulnerability
Age Matrix





Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

a firewall that is communicatively coupled with the at least one platform; at least one first data storage that is communicatively coupled with the at least one platform; and

at least one second data storage that is communicatively coupled with the at least one platform;

ManageEngine includes *a firewall that is communicatively coupled with the at least one platform* (e.g., The Firewall included in the ManageEngine platform); *at least one first data storage that is communicatively coupled with the at least one platform* (e.g., Vulnerability manager plus architecture comprises a central database for storing global vulnerabilities known as the Central Vulnerability Database); *and at least one second data storage that is communicatively coupled with the at least one platform* (e.g., the network devices or endpoints connected in the architecture of the vulnerability manager plus also acts as a storage device for local vulnerabilities and patches downloaded on the devices);

Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

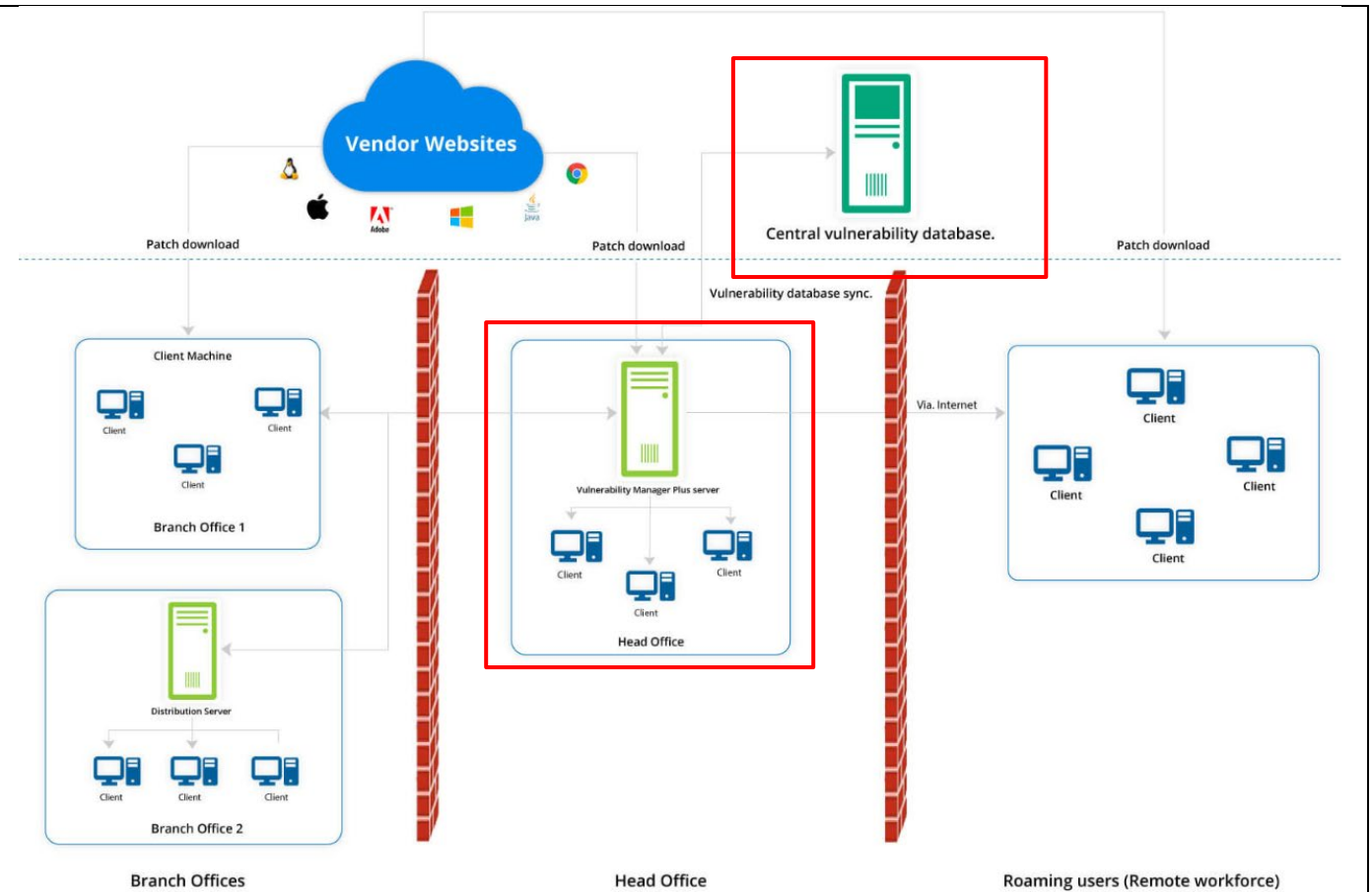
Assessing software vulnerabilities:

Vulnerability Manager Plus regularly scans your network for vulnerabilities. Once vulnerabilities are detected, then they are displayed in the web console. New vulnerabilities are being discovered constantly, therefore, it might get overwhelming for an user to decide on which vulnerability to remediate first. Therefore vulnerabilities should be assessed and prioritized based on the risk it presents to the enterprise. Vulnerability Manager Plus helps you assess the risk posed by vulnerabilities with the help of following parameters:

<https://www.manageengine.com/vulnerability-management/help/assess-and-remediate-vulnerabilities.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****3. Firewall Rule Reorder Recommendations**

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

	<p>Other features</p> <div> <div> <p>Firewall Reports</p> <p>Get a slew of security and traffic reports to asses the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.</p> </div> <div> <p>Firewall Log Management</p> <p>Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.</p> </div> <div> <p>Firewall Alerts</p> <p>Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.</p> </div> <div> <p>Firewall Compliance Management</p> <p>Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.</p> </div> <div> <p>Real-time Bandwidth Monitoring</p> <p>With live bandwidth monitoring, you can identify the abnormal sudden shhot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.</p> </div> <div> <p>Manage Firewall Service</p> <p>MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.</p> </div> </div> <p>https://www.manageengine.com/products/firewall/firewall-rule-management.html</p>
--	--

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of

privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

<https://www.manageengine.com/security.html?mesearch>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary

Zero-day
vulnerabilities

Vulnerability
Age Matrix

Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities		Vulnerable Software			
Vulnerabilities		Affected Systems	Exploit Status	Software Name	
	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)	
	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)	
	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)	
	Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)	

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<p>said at least one platform:</p> <p>receives a result of at least one operation performed on at least one of a plurality of networked devices, the at least one operation based on first information from the at least one first data storage identifying a plurality of potential vulnerabilities including at least one first potential vulnerability and at least one second potential vulnerability, the at least one operation configured for:</p>	<p>ManageEngine discloses that <i>the platform receives a result of at least one operation performed on at least one of a plurality of networked devices</i> (e.g., The vulnerability information collected by scanning operation), <i>the at least one operation based on first information from at least one first data storage identifying a plurality of potential vulnerabilities</i> (e.g., Known vulnerabilities) <i>including at least one first potential vulnerability and at least one second potential vulnerability</i> (e.g., Multiple vulnerability information collected from open source and stored in central database after verification and then system scan across multiple endpoints), <i>the at least one operation configured for:</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <div data-bbox="630 812 1123 855"> <p>2) What is Vulnerability Scanning?</p> </div> <div data-bbox="625 894 1887 1057" style="border: 1px solid red; padding: 10px;"> <p>Vulnerability scanning is a security process that checks your computer systems to find any weaknesses or vulnerabilities that could be used by hackers to gain unauthorized access. It's like a thorough check-up for your network and software, where any potential security risks are identified and reported back to you so that you can take action to fix them. This helps to protect your organization's digital assets and ensures that sensitive information remains secure.</p> </div> <p>https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html</p>
---	---

EXHIBIT 12

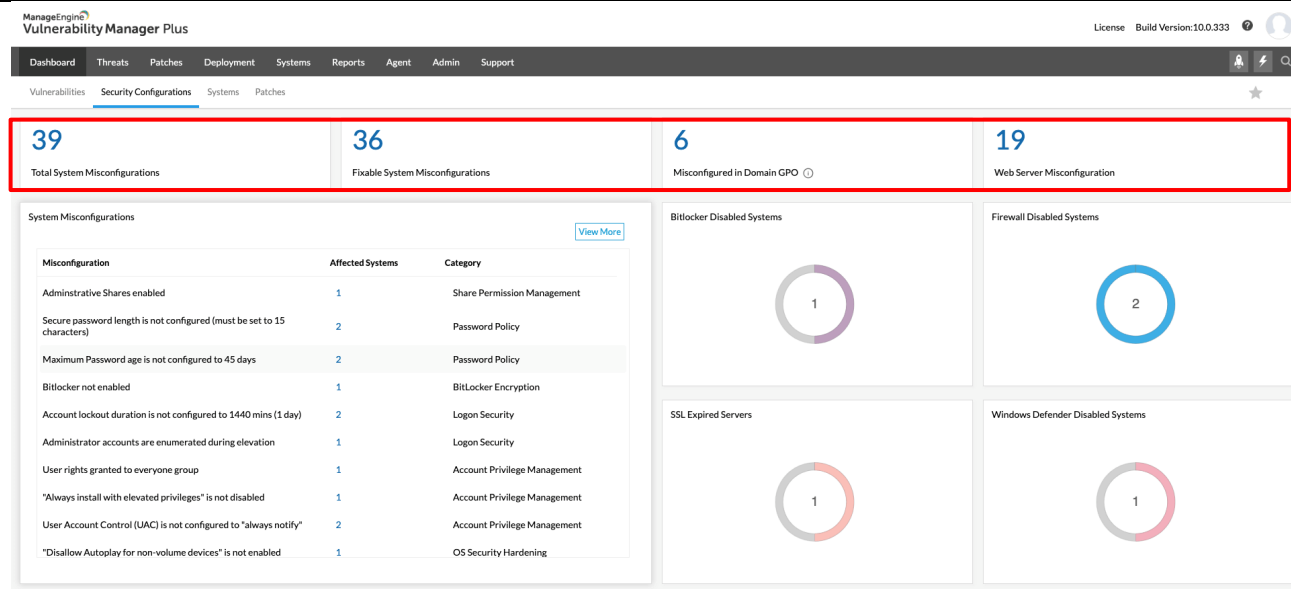
U.S. Patent No 10,154,055 v. Zoho

Comprehensive vulnerability scanning

Eliminating blind spots is the basis of successful **vulnerability management**. To achieve this, Vulnerability Manager Plus:

- Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems.
- Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move.
- Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more.

<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

Latest Vulnerabilities

Microsoft Vulnerabilities

Third Party Vulnerabilities

Web Server Vulnerabilities

DB Server Vulnerabilities

Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus interface. The top navigation bar includes links for Dashboard, Threats, Patches, Deployment, Systems, Reports, Agent, Admin, and Support. The left sidebar lists various threat categories: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations, High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area is titled 'This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.' It features a search bar with the text 'Search by CVE ID: CVE-XXXX-XXXX' and a filter dropdown set to 'Threat Category'. Below this is a table with columns: Threats, Threat Category, Affected Systems, and Action. The table lists five entries, including Google Chrome (x64) and various Internet Explorer security updates. Each entry has a 'Fix' button in the Action column. At the bottom right of the table, it shows '1 - 5 of 5' and a page size selector set to '30'.

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721_6_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

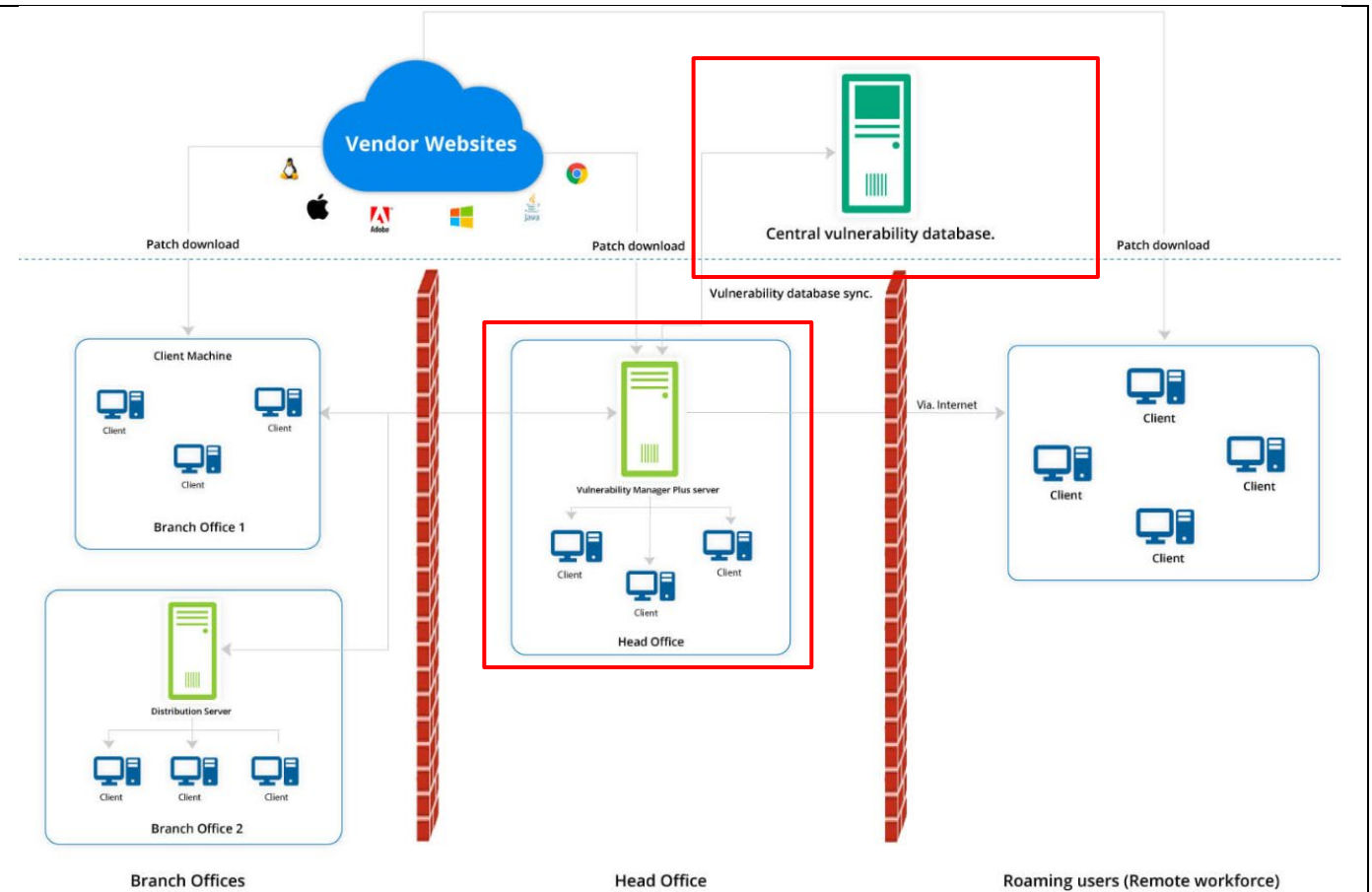
Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Vulnerability Manager Plus Server:

The Vulnerability Manager Plus Server helps you to centrally perform all the vulnerability management and compliance tasks in your network endpoints. Some of the tasks include the following:

- Installing agents in computers
- Scanning computers for vulnerabilities and misconfigurations
- Deploying patches and secure configurations
- Uninstalling high-risk software
- Auditing active ports
- Auditing for compliance against CIS benchmarks

Any of the Windows computers in your network with the requirements mentioned [here](#) can be hosted as your Vulnerability Manager Plus Server. This Vulnerability Manager Plus Server at the customer site subscribes to the Central Vulnerability Database, from which it synchronizes the latest information on threats, patches, vulnerabilities, and compliance policies. Patches are downloaded directly from vendor sites and stored centrally in the server's patch store and will be replicated to your network endpoints to conserve bandwidth.

<https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html#v1>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary

Zero-day
vulnerabilities

Vulnerability
Age Matrix





Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

	<p>Intrusion detection and prevention</p> <p>Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.</p> <p>At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.</p> <p>https://www.manageengine.com/security.html?mesearch</p>
<p>identifying at least one configuration associated with the at least one networked device, and</p>	<p>ManageEngine <i>identifying at least one configuration associated with the at least one networked device</i> (e.g., The vulnerability information collected by scanning operation and identify a misconfiguration).</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****How to prevent security misconfigurations?**

If vulnerabilities are the gateway to the network, it's the misconfigurations that attackers leverage to worm their way to the intended targets. Security misconfigurations are not hard to fix, but they are unavoidable in an enterprise operating at scale. Finding them is a needle in the haystack, as they can be located across any component in an organization's systems, such as its servers, operating systems, applications, and browsers. Lack of visibility and centralized means to remediate misconfigurations makes organizations fall victim to misconfiguration attacks.

<https://www.manageengine.com/vulnerability-management/misconfiguration/?meseach>

As soon as it's up and running in your network, Vulnerability Manager Plus automatically discovers your Active Directory and workgroup assets. Scaling up? No problem. Since Vulnerability Manager Plus is constantly in sync with Active

Directory, new assets will be brought under management as soon as they enter your network, leaving no opportunity for new threats to go unnoticed.

Leveraging endpoint agent technology, Vulnerability Manager Plus scans your laptops, desktops, servers, databases, workstations, and virtual machines across your entire global hybrid IT environment every 90 minutes, irrespective of whether they're within the corporate boundary or not.

You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ.

Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation.

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

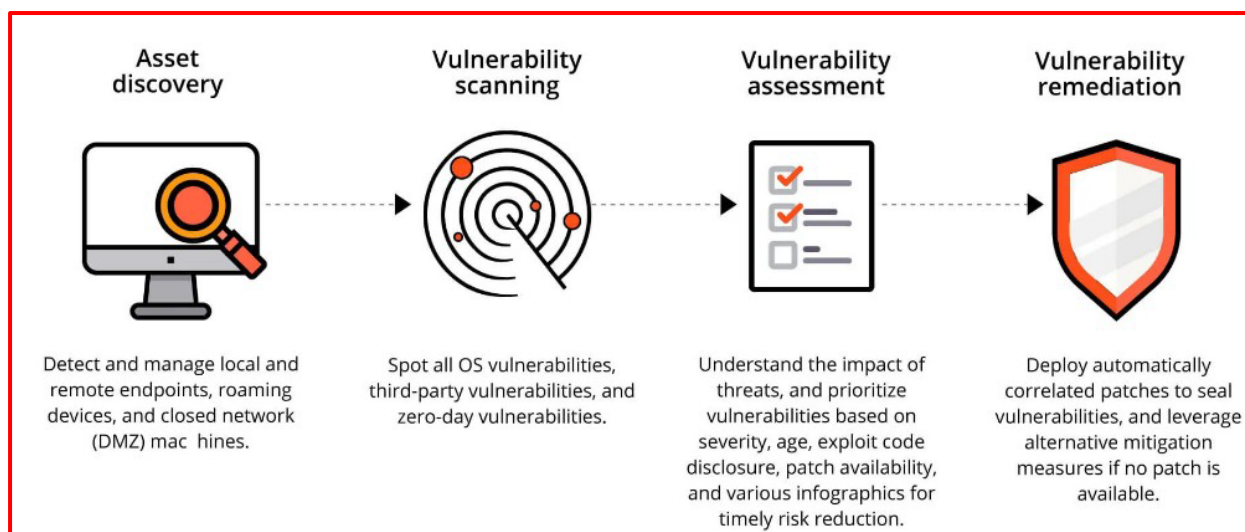
	https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html
determining that the at least one networked device is actually vulnerable to at least one actual vulnerability, based on the identified at least one configuration and the first information from the at least one first data storage identifying the plurality of potential vulnerabilities, such that second information associated with the result is stored in the at least one second data storage separate from the at least one first data storage, the second information relating to the at least one actual vulnerability to which the at least one	<p>ManageEngine includes <i>determining that the at least one networked device is actually vulnerable to at least one actual vulnerability</i> (e.g., The vulnerability information collected by scanning operation and identify a misconfiguration), <i>based on the identified at least one configuration and the first information from the at least one first data storage identifying the plurality of potential vulnerabilities</i> (e.g., Multiple vulnerability information collected from open source and stored in central database after verification). <i>such that second information associated with the result is stored in the at least one second data storage separate from the at least one first data storage, the second information relating to the at least one actual vulnerability to which the at least one networked device is actually vulnerable</i> (e.g., The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and if vulnerabilities exist then displays them in a dedicated view in the console with its fix);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

networked device is actually vulnerable;

What are the 4 steps in vulnerability assessment?

Vulnerability Manager Plus is a well-rounded vulnerability assessment tool that regularly scans your network for vulnerabilities, delivers insights into risk, and helps close the vulnerability management loop instantly with direct remediation from the console.



<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****Leverage a dedicated view for zero-days**

ManageEngine's security researchers constantly probe the internet for any details regarding new threats. As soon as details regarding zero-day vulnerabilities and publicly disclosed vulnerabilities come to light, the information is verified and updated to the central vulnerability database at once, and the data is synchronized to the Vulnerability Manager Plus server.

The screenshot shows the ManageEngine Vulnerability Manager Plus dashboard. The left sidebar contains navigation options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations, High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area is titled 'Threats' and includes a sub-header: 'This view displays zero day vulnerabilities like Wannacry, Meltdown and Spectre, etc. that are present in your network.' Below this, there is a filter section with 'Filter by: Threat Categ...' and a search bar 'Search by CVE ID: CVE-XXXX-XXXX'. A table displays the following data:

Threats	Threat Category	Affected Systems	Action
Google Chrome (x64) (78.0.3904.87)	ZeroDay_CVE-2019-13721&_CVE-2019-...	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2019-09 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	CVE-2019-13675/CVE-2019-1235	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 9 for Windows Server 200...	IE_ZeroDay_CVE-2018-8653	1	Fix
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 20...	IE_ZeroDay_CVE-2018-8653	1	Fix

At the bottom right of the table, it says '1 - 5 of 5' and '30'.

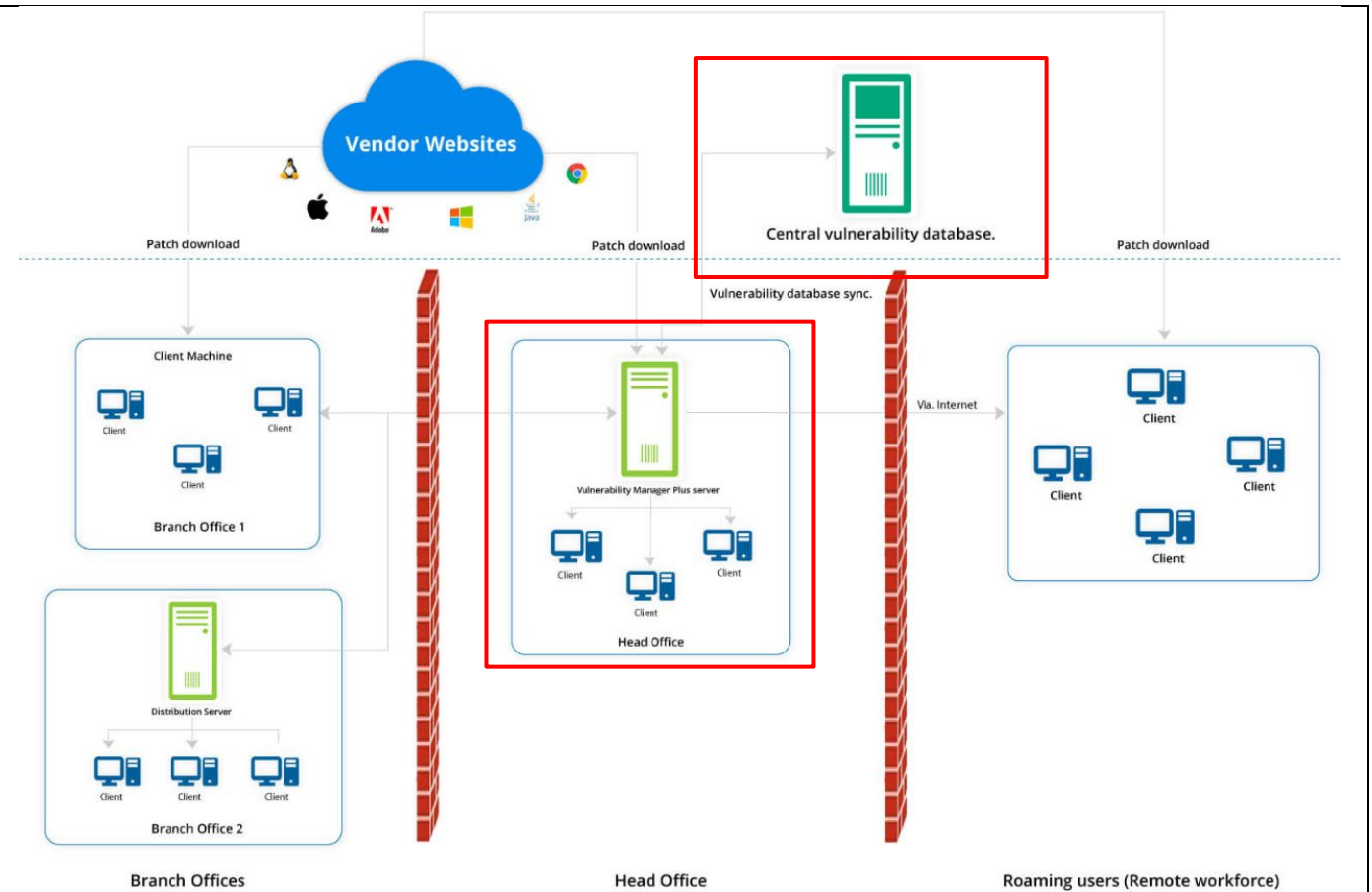
Vulnerability Manager Plus then scans your network for zero-day vulnerabilities and displays them in a dedicated view in the console, preventing them from being jumbled with less critical vulnerabilities. One of the components in the vulnerability dashboard keeps you constantly informed of how many zero-day vulnerabilities remain unresolved in your network.

Furthermore, you can learn in detail about the latest zero-day vulnerability from tech articles available in the security newsfeed. [Subscribe](#) to the Vulnerability Manager Plus pitstop to receive email notifications on the latest zero day attacks and related news

<https://www.manageengine.com/vulnerability-management/zero-day-vulnerability-mitigation.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho



<https://www.manageengine.com/vulnerability-management/images/vulnerability-management-process.jpg>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary

Zero-day
vulnerabilities

Vulnerability
Age Matrix





Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

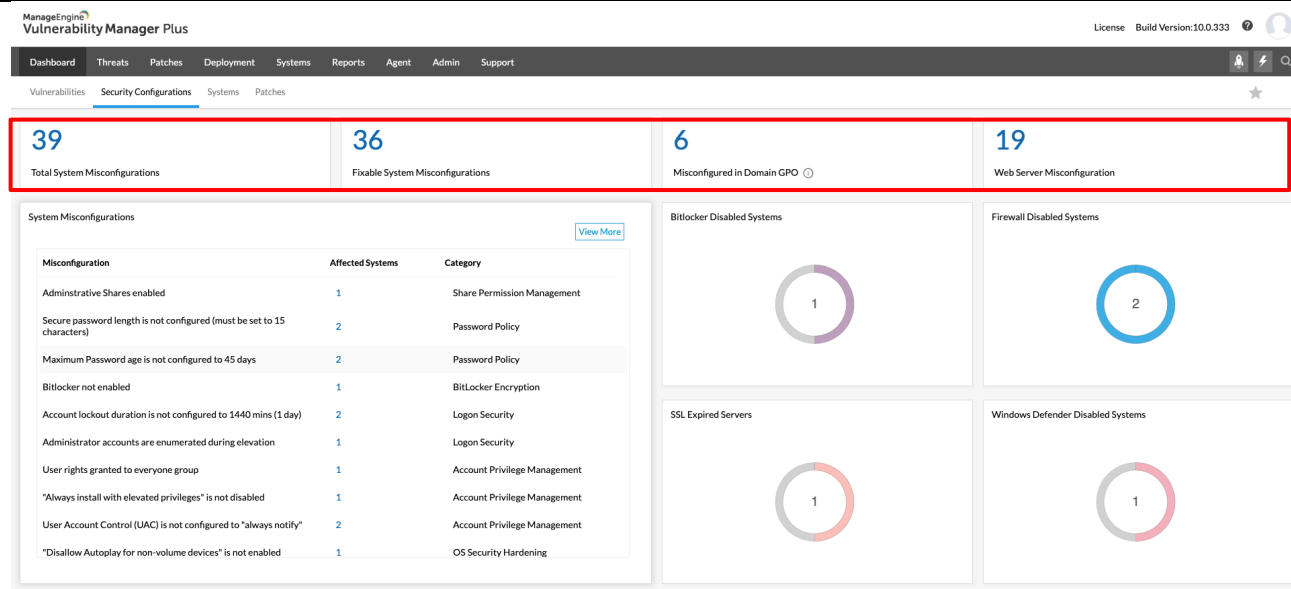
Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

Latest Vulnerabilities

Microsoft Vulnerabilities

Third Party Vulnerabilities

Web Server Vulnerabilities

DB Server Vulnerabilities

Last updated on **May 7, 2024**

S.No	Vulnerability Name	Severity
1	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x64)	Important
2	Vulnerabilities CVE-2024-4331,CVE-2024-4368 are fixed in Microsoft Edge for chromium business (124.0.2478.80) (x86)	Important
3	Vulnerabilities CVE-2020-1968 are fixed in Duo Security Authentication Proxy 5.0.2	Low
4	Vulnerabilities CVE-2021-1492 are fixed in Duo Security Authentication Proxy (5.2.0)	Important
5	Vulnerabilities CVE-2020-1971 are fixed in Duo Security Authentication Proxy (5.4.1)	Moderate
6	Vulnerabilities CVE-2022-0778 are fixed in Duo Security Authentication Proxy (5.6.0)	Important
7	Vulnerabilities CVE-2022-0778,CVE-2022-21712 are fixed in Duo Security Authentication Proxy (5.6.1)	Critical

<https://www.manageengine.com/vulnerability-management/vulnerability-database/>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

How to prevent security misconfigurations?

If vulnerabilities are the gateway to the network, it's the misconfigurations that attackers leverage to worm their way to the intended targets. Security misconfigurations are not hard to fix, but they are unavoidable in an enterprise operating at scale. Finding them is a needle in the haystack, as they can be located across any component in an organization's systems, such as its servers, operating systems, applications, and browsers. Lack of visibility and centralized means to remediate misconfigurations makes organizations fall victim to misconfiguration attacks.

<https://www.manageengine.com/vulnerability-management/misconfiguration/?meseach>

| How can I view the complete list of CVEs affecting my endpoints?

Vulnerability Manager Plus boasts a dedicated Detected CVEs view that lists all the CVEs affecting your network endpoints. All you have to do is select the desired CVEs then click Fix CVE to instantly create a patch deployment task in all the affected machines.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

	<p>As soon as it's up and running in your network, Vulnerability Manager Plus automatically discovers your Active Directory and workgroup assets. Scaling up? No problem. Since Vulnerability Manager Plus is constantly in sync with Active Directory, new assets will be brought under management as soon as they enter your network, leaving no opportunity for new threats to go unnoticed.</p> <p>Leveraging endpoint agent technology, Vulnerability Manager Plus scans your laptops, desktops, servers, databases, workstations, and virtual machines across your entire global hybrid IT environment every 90 minutes, irrespective of whether they're within the corporate boundary or not.</p> <p>You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ.</p> <p>Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation.</p> <p>https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html</p>
<p>causes to display, via at least one user interface, a plurality of techniques including a first technique for utilizing the intrusion prevention system component for occurrence mitigation, and a second</p>	<p>ManageEngine <i>causes to display, via at least one user interface</i> (e.g., ManageEngine Vulnerability Manager Plus includes web consol), <i>a plurality of techniques including a first technique for utilizing an intrusion prevention system component for occurrence mitigation</i> (e.g., ManageEngine Vulnerability Manager Plus includes antivirus option), <i>and a second technique for utilizing a firewall for occurrence mitigation</i> (e.g., ManageEngine Vulnerability Manager Plus includes firewall option. The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements);</p>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

<p>technique for utilizing the firewall for occurrence mitigation;</p>	<p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Intrusion detection and prevention</p> <p>Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.</p> <p>At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.</p> <p>https://www.manageengine.com/security.html?mesearch</p>
--	--

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary

Zero-day
vulnerabilities

Vulnerability
Age Matrix





Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

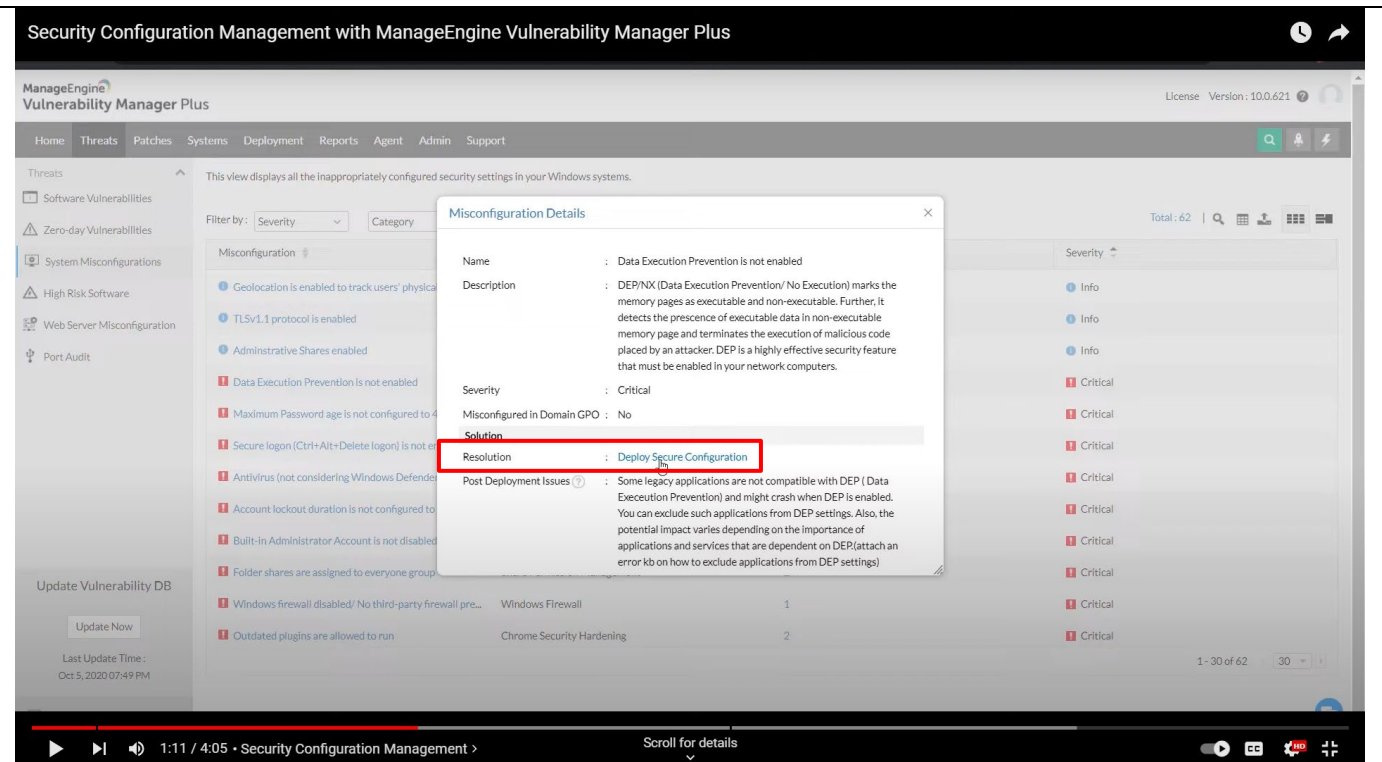
<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

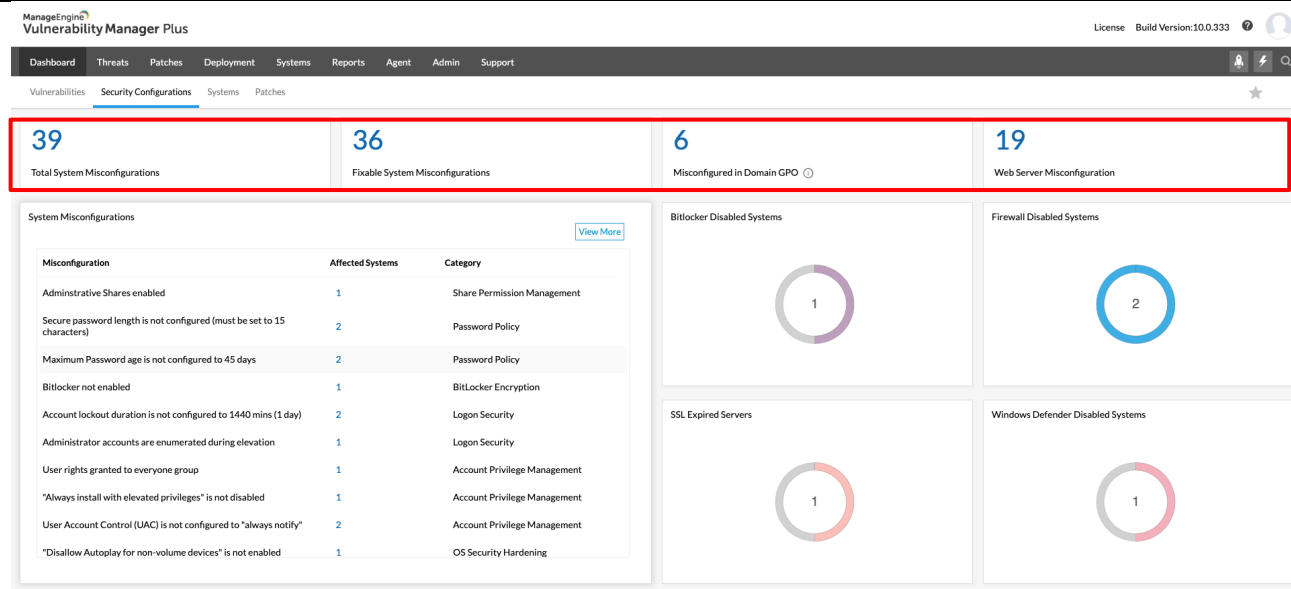
The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations (selected), High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area shows a list of misconfigurations. A filter dropdown is open, showing categories like Antivirus Protection, User Account Management, Windows Firewall (highlighted with a red box), Password Policy, SSL and TLS Security, and Chrome Security Hardening. The list of misconfigurations includes items like 'Geolocation is enabled to track', 'TLSv1.1 protocol is enabled', 'Administrative Shares enabled', 'Data Execution Prevention is enabled', 'Maximum Password age is not configured to 45 days', 'Secure logon (Ctrl+Alt+Delete logon) is not enabled', 'Antivirus (not considering Windows Defender) not installed', 'Account lockout duration is not configured to 1440 minutes', 'Built-in Administrator Account is not disabled', 'Folder shares are assigned to everyone group', 'Windows firewall disabled/ No third-party firewall pre...' (highlighted with a red box and marked as Critical), and 'Outdated plugins are allowed to run'.

Misconfiguration	Category	Affected Systems	Severity
Geolocation is enabled to track	User Account Management	2	Info
TLSv1.1 protocol is enabled	Windows Firewall	1	Info
Administrative Shares enabled	Password Policy	3	Info
Data Execution Prevention is enabled	SSL and TLS Security	4	Critical
Maximum Password age is not configured to 45 days	Chrome Security Hardening	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Password Policy	1	Critical
Antivirus (not considering Windows Defender) not installed	Logon Security	1	Critical
Account lockout duration is not configured to 1440 minutes	Antivirus Protection	2	Critical
Built-in Administrator Account is not disabled	Logon Security	2	Critical
Folder shares are assigned to everyone group	User Account Management	2	Critical
Windows firewall disabled/ No third-party firewall pre...	Share Permission Management	2	Critical
Outdated plugins are allowed to run	Windows Firewall	1	Critical
	Chrome Security Hardening	2	Critical

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****3. Firewall Rule Reorder Recommendations**

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

	<p>Other features</p> <div> <div> <p>Firewall Reports</p> <p>Get a slew of security and traffic reports to asses the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.</p> </div> <div> <p>Firewall Log Management</p> <p>Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.</p> </div> <div> <p>Firewall Alerts</p> <p>Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.</p> </div> <div> <p>Firewall Compliance Management</p> <p>Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.</p> </div> <div> <p>Real-time Bandwidth Monitoring</p> <p>With live bandwidth monitoring, you can identify the abnormal sudden shhot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.</p> </div> <div> <p>Manage Firewall Service</p> <p>MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.</p> </div> </div> <p>https://www.manageengine.com/products/firewall/firewall-rule-management.html</p>
--	--

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the 'Install/Uninstall Windows Patch (Computer)' configuration page in the ManageEngine Vulnerability Management console. The interface includes a left-hand navigation menu with options like 'Home', 'Threats', 'Patches', 'Systems', 'Deployment', 'Agents', 'Reports', 'Admin', and 'Support'. The main content area is divided into several sections:

- Name and Description:** A text field for 'Name' (currently 'No Configuration') and a link to 'Add Description'.
- Install Patch:** A section for configuring the patch operation, including 'Operation Type' (radio buttons for 'Install Patch' and 'Uninstall Patch'), and a table of installed patches.
- Schedule Settings (Optional):** Checkboxes for 'Install on the fly' and 'Do not apply Windows configuration after the time specified below'.
- Deployment Rule:** A checkbox for 'Continue deployment even if some patches cannot be downloaded'.
- Deployment Settings:** A dropdown for 'Apply Deployment Policy' and a link to 'Create Patch Policy'.
- Define Target:** A section for selecting targets, including 'Remote Office Domain' and 'Local Office'.
- Execution Settings (Optional):** A section for configuring execution parameters.

The table of installed patches shows the following data:

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
10340	Security Update for Windows 8.1 KB3033970	Yes/No/Yes	Security Update	Approved	1	0	Re
10340	Security Update for Windows 8.1 KB3033970	Yes/No/Yes	Security Update	Approved	1	0	Re

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

How can I access drilled-down information on vulnerabilities in individual systems?

Clicking on a system takes you to a drilled-down view that clusters vulnerabilities of the system into three major categories:

The screenshot shows the ManageEngine Vulnerability Assessment interface. The left sidebar contains navigation options like 'System Health Summary', 'Highly Vulnerable Systems', 'Vulnerable Systems', 'Healthy Systems', 'System Health Policy', 'Managed Systems', 'Scan Systems', 'By Patches', 'By Vulnerabilities', 'By Misconfigurations', 'By Web Server Misconfiguration', 'By High Risk Software', 'Attention Required', and 'Windows 10 EOL Systems'. The main content area is titled 'suraj-7073' and shows a 'Vulnerabilities' section. The 'Web' tab is selected, displaying a table of vulnerabilities. The table has columns for 'Vulnerabilities', 'File Path', 'Exploit Status', 'Patch Availability', 'CVSS 3.0 Score', and 'CVSS 2.0 Score'. Three vulnerabilities are listed, all with an exploit status of 'Not available' and a patch availability of 'Not available'.

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score
Vulnerabilities CVE-2020-17527 are fixed in 17 November...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2020-17527,CVE-2021-24122 are fix...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2021-25329,CVE-2020-9484,CVE-20...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	6.9	7.5

- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<p>allows receipt of:</p> <p>user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation;</p> <p>user input causing selection of the second technique for utilizing the firewall for occurrence mitigation;</p>	<p>ManageEngine <i>allows receipt, user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation</i> (e.g., ManageEngine Vulnerability Manager Plus includes web consol on which user can select antivirus option); <i>user input causing selection of the second technique for utilizing the firewall for occurrence mitigation</i> (e.g., ManageEngine Vulnerability Manager Plus includes firewall option. The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements);</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>Intrusion detection and prevention</p> <p>Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.</p> <p>At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.</p>
---	--

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<https://www.manageengine.com/security.html?mearch>

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary

Zero-day
vulnerabilities

Vulnerability
Age Matrix





Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

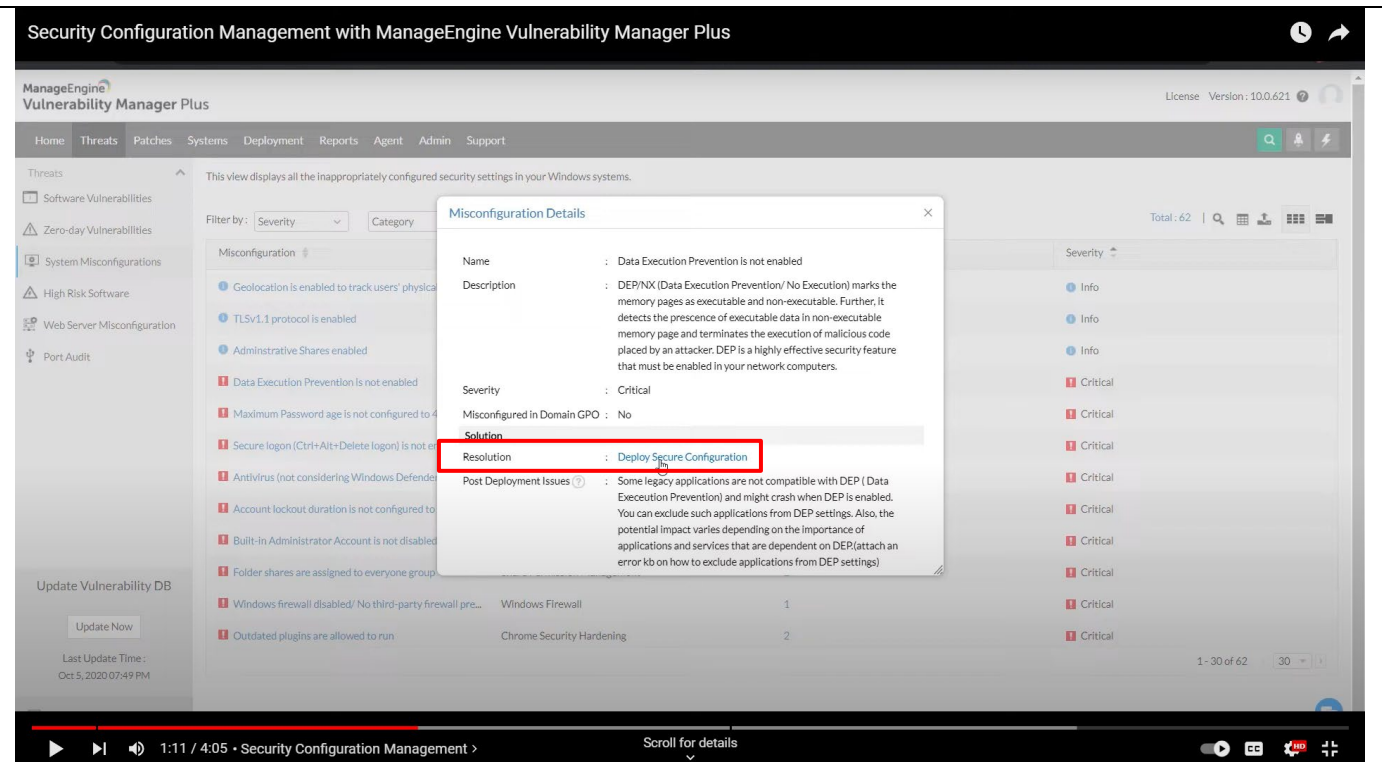
<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

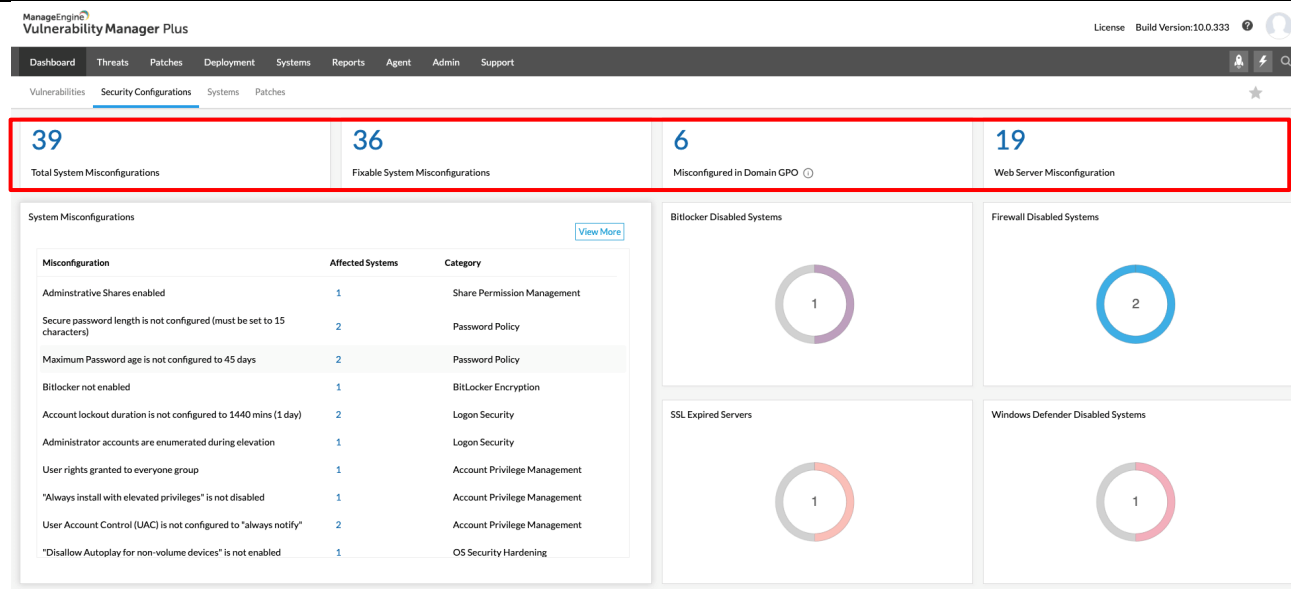
The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Home, Threats, Patches, Systems, Deployment, Reports, Agent, Admin, and Support. The main content area is titled 'This view displays all the inappropriately configured security settings in your Windows systems.' It features a table of misconfigurations with columns for Category, Affected Systems, and Severity. A filter dropdown is open, showing 'Windows Firewall' selected. The table lists various security settings, with the entry 'Windows firewall disabled/ No third-party firewall pre...' highlighted in red, indicating a critical issue.

Category	Affected Systems	Severity
Geolocation is enabled to track	2	Info
TLSv1.1 protocol is enabled	1	Info
Administrative Shares enabled	3	Info
Data Execution Prevention is disabled	4	Critical
Maximum Password age is not configured to 45 days	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	1	Critical
Antivirus (not considering Windows Defender) not installed	1	Critical
Account lockout duration is not configured to 1440 minutes	2	Critical
Built-in Administrator Account is not disabled	2	Critical
Folder shares are assigned to everyone group	2	Critical
Windows firewall disabled/ No third-party firewall pre...	1	Critical
Outdated plugins are allowed to run	2	Critical

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****3. Firewall Rule Reorder Recommendations**

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

	<div data-bbox="644 235 926 276" data-label="Section-Header"> <p>Other features</p> </div> <div data-bbox="644 318 886 355" data-label="Section-Header"> <p>Firewall Reports</p> </div> <div data-bbox="644 363 1222 527" data-label="Text"> <p>Get a slew of security and traffic reports to asses the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.</p> </div> <div data-bbox="644 571 1022 610" data-label="Section-Header"> <p>Firewall Log Management</p> </div> <div data-bbox="644 617 1213 782" data-label="Text"> <p>Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.</p> </div> <div data-bbox="644 812 858 844" data-label="Section-Header"> <p>Firewall Alerts</p> </div> <div data-bbox="644 854 1220 1018" data-label="Text"> <p>Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.</p> </div> <div data-bbox="1276 326 1785 365" data-label="Section-Header"> <p>Firewall Compliance Management</p> </div> <div data-bbox="1276 381 1887 547" data-label="Text"> <p>Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.</p> </div> <div data-bbox="1276 571 1757 610" data-label="Section-Header"> <p>Real-time Bandwidth Monitoring</p> </div> <div data-bbox="1276 617 1850 782" data-label="Text"> <p>With live bandwidth monitoring, you can identify the abnormal sudden shhot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.</p> </div> <div data-bbox="1276 812 1640 844" data-label="Section-Header"> <p>Manage Firewall Service</p> </div> <div data-bbox="1276 854 1883 1018" data-label="Text"> <p>MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.</p> </div> <div data-bbox="562 1050 1625 1089" data-label="Text"> <p>https://www.manageengine.com/products/firewall/firewall-rule-management.html</p> </div>
--	--

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the 'Install/Uninstall Windows Patch (Computer)' configuration page in the ManageEngine Vulnerability Management console. The left sidebar shows navigation options like Home, Threats, Patches, Systems, Deployment, Agents, Reports, Admin, and Support. The main content area is divided into several sections:

- Name and Description:** A text input field for 'Name' (currently 'No Configuration') and a link to 'Add Description'.
- Install Patch:** A section with 'Operation Type' (radio buttons for 'Install Patch' and 'Uninstall Patch'), a '+ Add Patch' link, and a table of installed patches.
- Scheduler Settings (Optional):** Checkboxes for 'Install Only' and 'Do not apply Windows Configuration after the time specified below'.
- Deployment Rule:** A checkbox for 'Continue deployment even if some patches cannot be downloaded' with a note about failed patches.
- Deployment Settings:** A dropdown for 'Apply Deployment Policy' and a '+ Create Policy' link.
- Define Targets:** A section for 'Target 1' with 'Remote Office Domain' and 'Local Office' tabs. It includes a 'Filter Computers based on' dropdown (set to 'Computer'), a 'Domain' input field (set to 'SECURITY-WEB-02'), and an 'Exclude Target' dropdown (set to 'Select').
- Execution Settings (Optional):** A section at the bottom for further configuration.

At the bottom left, there is a 'Update Vulnerability DB' button and a 'Last Update Time' of 'JUL 23 2024 10:03 AM'.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

How can I access drilled-down information on vulnerabilities in individual systems?

Clicking on a system takes you to a drilled-down view that clusters vulnerabilities of the system into three major categories:

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score
Vulnerabilities CVE-2020-17527 are fixed in 17 November...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2020-17527,CVE-2021-24122 are fix...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2021-25329,CVE-2020-9484,CVE-20...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	6.9	7.5

- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<p>applies, based on the user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation, the first technique for utilizing the intrusion prevention system component for occurrence mitigation;</p> <p>applies, based on the user input causing selection of the second technique for utilizing the firewall for occurrence mitigation, the second technique for utilizing the firewall for occurrence mitigation;</p>	<p><i>ManageEngine applies, based on the user input causing selection of the first technique for utilizing the intrusion prevention system component for occurrence mitigation, the first technique for utilizing the intrusion prevention system component for occurrence mitigation (e.g., ManageEngine Vulnerability Manager Plus includes web consol on which user can select antivirus option); applies, based on the user input causing selection of the second technique for utilizing the firewall for occurrence mitigation, the second technique for utilizing the firewall for occurrence mitigation (e.g., ManageEngine Vulnerability Manager Plus includes firewall option. The ManageEngine provides flexibility to choose the devices for applying the different policies or mitigation techniques according to the requirements);</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of

privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

<https://www.manageengine.com/security.html?mesearch>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

See what matters most at a glimpse with dashboard widgets

The vulnerability information collected across multiple endpoints is consolidated in a web console for centralized management and represented with meaningful context in dashboard widgets, translating to reliable and timely results.

These interactive dashboard widgets are tailored to direct your attention to the most alarming areas in your network.

Vulnerability Severity
Summary

Zero-day
vulnerabilities

Vulnerability
Age Matrix





Vulnerabilities
Over Time

**High Priority
Vulnerabilities**

High Priority Vulnerabilities: Where your primary focus should be!

Vulnerabilities Vulnerable Software

[View More](#)

Vulnerabilities	Affected Systems	Exploit Status	Software Name
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Enterprise Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Basic Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Home Premium Edition (x64)
 Security Update for Windows 8.1 for x64-based Systems (KB3010788)	1	Available	Windows 8.1 Professional Edition (x64)

Vulnerability Manager Plus automatically curates a list of vulnerabilities that are on the verge of exploitation. This list takes various risk factors into account, such as how easily exploitable a vulnerability is, its severity, age, and patch availability. This table helps you ensure that you haven't left out any essentials in your [vulnerability assessment process](#).

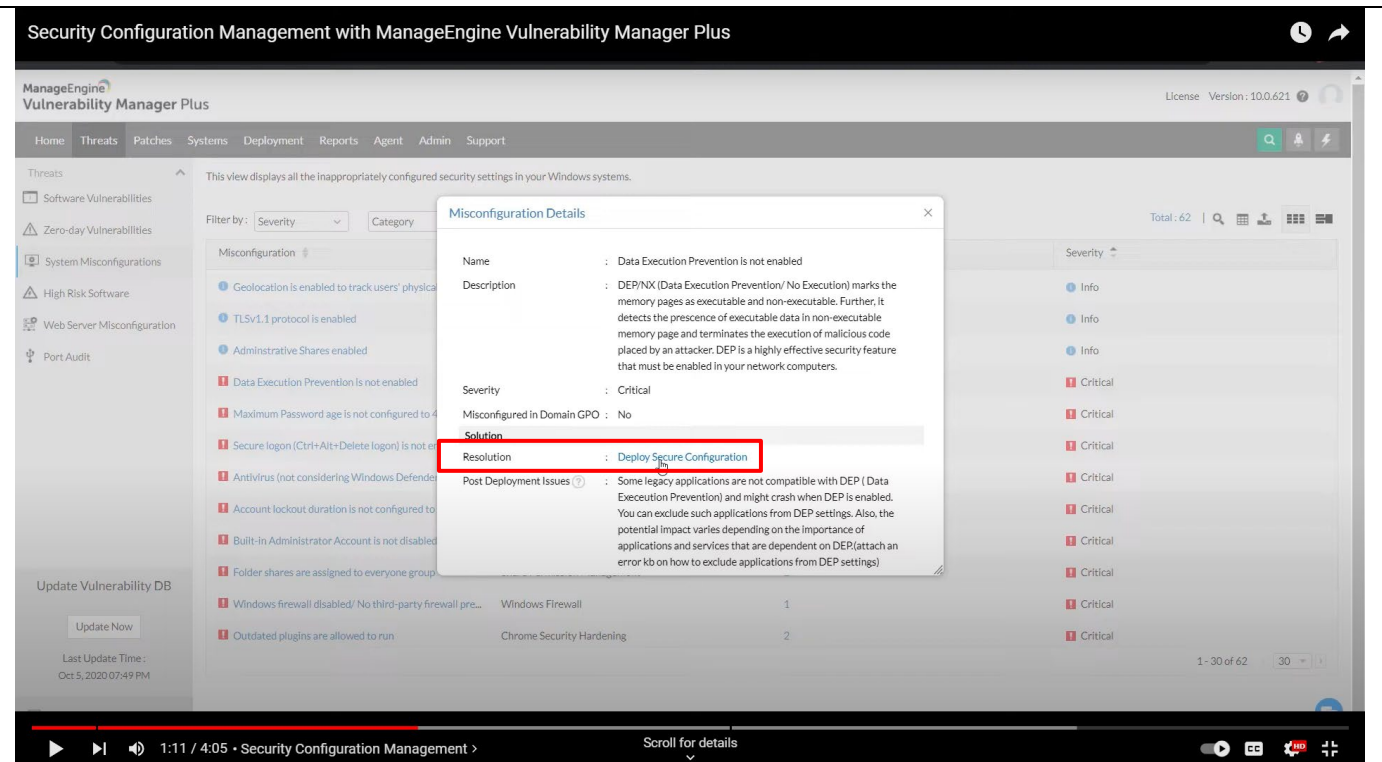
<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

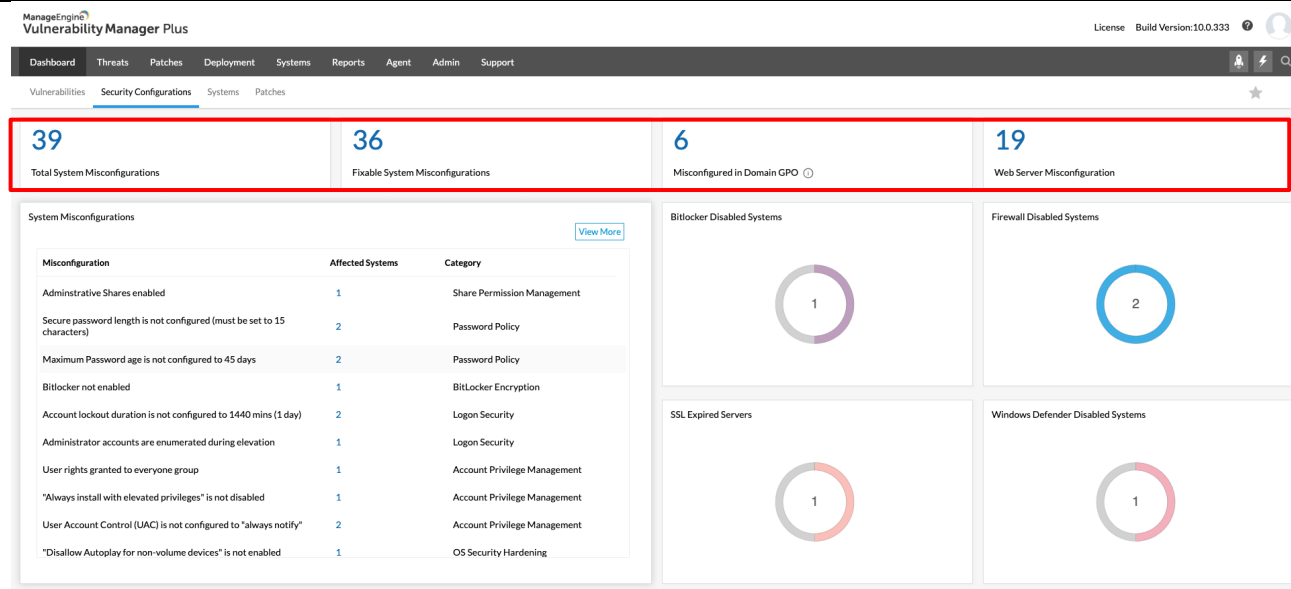
The screenshot displays the ManageEngine Vulnerability Manager Plus interface. The left sidebar shows navigation options: Threats, Software Vulnerabilities, Zero-day Vulnerabilities, System Misconfigurations (selected), High Risk Software, Web Server Misconfiguration, and Port Audit. The main content area shows a list of misconfigurations. A filter dropdown is open, showing categories like Antivirus Protection, User Account Management, Windows Firewall (highlighted with a red box), Password Policy, SSL and TLS Security, and Chrome Security Hardening. The list of misconfigurations includes items like 'Geolocation is enabled to track', 'TLSv1.1 protocol is enabled', 'Administrative Shares enabled', 'Data Execution Prevention is not enabled', 'Maximum Password age is not configured to 45 days', 'Secure logon (Ctrl+Alt+Delete logon) is not enabled', 'Antivirus (not considering Windows Defender) not installed', 'Account lockout duration is not configured to 1440 minutes', 'Built-in Administrator Account is not disabled', 'Folder shares are assigned to everyone group', 'Windows firewall disabled/ No third-party firewall pre...' (highlighted with a red box and marked as Critical), and 'Outdated plugins are allowed to run'.

Misconfiguration	Category	Affected Systems	Severity
Geolocation is enabled to track	User Account Management	2	Info
TLSv1.1 protocol is enabled	Windows Firewall	1	Info
Administrative Shares enabled	Password Policy	3	Info
Data Execution Prevention is not enabled	Chrome Security Hardening	4	Critical
Maximum Password age is not configured to 45 days	Password Policy	1	Critical
Secure logon (Ctrl+Alt+Delete logon) is not enabled	Logon Security	1	Critical
Antivirus (not considering Windows Defender) not installed	Antivirus Protection	1	Critical
Account lockout duration is not configured to 1440 minutes	Logon Security	2	Critical
Built-in Administrator Account is not disabled	User Account Management	2	Critical
Folder shares are assigned to everyone group	Share Permission Management	2	Critical
Windows firewall disabled/ No third-party firewall pre...	Windows Firewall	1	Critical
Outdated plugins are allowed to run	Chrome Security Hardening	2	Critical

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=98s>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<https://www.youtube.com/watch?v=p2Oh87NruMo&t=53s>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****3. Firewall Rule Reorder Recommendations**

Policy Name	Rule Name	Position (From - To)	Hit Count	Perf. Improvement
Outside_Access_In	2	2 → 1	55	100
Inside_Access_Out	7	9 → 4	19	100
Inside_Access_Out	8	10 → 5	35	100

Firewall Analyzer analyzes various rule interactions and anomalies to provide suggestions on rule position. By correlating the number of rule hits with rule complexity and anomalies, it can estimate the performance improvement for a suggested change. With the help of this report, you get an understanding of how to organize firewall rules to maximize speed.

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

	<p>Other features</p> <div> <div> <p>Firewall Reports</p> <p>Get a slew of security and traffic reports to asses the network security posture. Analyze the reports and take measures to prevent future security incidents. Monitor the Internet usage of enterprise users.</p> </div> <div> <p>Firewall Log Management</p> <p>Unlock the wealth of network security information hidden in the firewall logs. Analyze the logs to find the security threats faced by the network. Also, get the Internet traffic pattern for capacity planning.</p> </div> <div> <p>Firewall Alerts</p> <p>Take instant remedial actions, when you get notified in real-time for network security incidents. Check and restrict Internet usage if bandwidth exceeds specified threshold.</p> </div> <div> <p>Firewall Compliance Management</p> <p>Integrated compliance management system automates your firewall compliance audits. Ready made reports available for the major regulatory mandates such as PCI-DSS, ISO 27001, NIST, NERC-CIP, and SANS.</p> </div> <div> <p>Real-time Bandwidth Monitoring</p> <p>With live bandwidth monitoring, you can identify the abnormal sudden shhot up of bandwidth use. Take remedial measures to contain the sudden surge in bandwidth consumption.</p> </div> <div> <p>Manage Firewall Service</p> <p>MSSPs can host multiple tenants, with exclusive segmented and secured access to their respective data. Scalable to address their needs. Manages firewalls deployed around the globe.</p> </div> </div> <p>https://www.manageengine.com/products/firewall/firewall-rule-management.html</p>
--	--

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the 'Install/Uninstall Windows Patch (Computer)' configuration page in the ManageEngine Vulnerability Management console. The left sidebar shows navigation options like Home, Threats, Patches, Systems, Deployment, Agents, Reports, Admin, and Support. The main content area is divided into several sections:

- Name and Description:** Includes a 'Name' field with the value 'NoConfiguredPDS' and an 'Add Description' button.
- Install Patch:** Features a 'Use of Patches' section with radio buttons for 'Install Patch' (selected) and 'Uninstall Patch'. Below this is a table listing patches.

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
16340	Security Update for Windows 8 KB3033970	After Patching	Security Update	Approved	1	0	R
27504	Security Update for Windows 8 KB3033970	After Patching	Security Update	Approved	1	0	R
- Scheduler Settings (Optional):** Includes checkboxes for 'Install after' and 'Do not apply Windows configuration after the time specified below'. A 'Deployment Rule' section has a checkbox for 'Continue deployment even if some patches cannot be downloaded'.
- Deployment Settings:** Includes a 'Apply Deployment Policy' dropdown menu set to 'Select Policy' and a 'Create Policy' button.
- Define Targets:** Includes a 'Target 1' section with a 'Remote Office Domain' and a 'Local Office' section. The 'Local Office' section has a 'Filter Computers based on' dropdown set to 'Computer' and a 'Domain' field set to 'SECURITY-WEB-02'. There is also an 'Exclude Target' section with a 'Domain' dropdown set to 'Select'.
- Execution Settings (Optional):** Includes a 'Filter' button.

At the bottom left, there is a 'Update Vulnerability DB' button and a 'Last Update Time: JUL 25 10:03 AM' timestamp.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

How can I access drilled-down information on vulnerabilities in individual systems?

Clicking on a system takes you to a drilled-down view that clusters vulnerabilities of the system into three major categories:

The screenshot displays the ManageEngine Vulnerability Assessment interface. The left sidebar contains navigation options such as 'System Health Summary', 'Highly Vulnerable Systems (3)', 'Vulnerable Systems (1)', 'Healthy Systems (6)', 'System Health Policy', 'Managed Systems', 'Scan Systems (13)', 'By Patches', 'By Vulnerabilities (7)', 'By Misconfigurations (8)', 'By Web Server Misconfiguration (5)', 'By High Risk Software (7)', 'Attention Required', 'Windows 10 EOL Systems', and 'Update Vulnerability DB'. The main content area is titled 'suraj-7073' and includes tabs for 'Summary', 'Installed Software', 'Vulnerabilities', 'Patches', 'Security Config', and 'Port Audit'. The 'Vulnerabilities' tab is active, showing a table of vulnerabilities. The table has columns for 'Vulnerabilities', 'File Path', 'Exploit Status', 'Patch Availability', 'CVSS 3.0 Score', and 'CVSS 2.0 Score'. There are three rows of data, all showing 'Not available' for exploit status and patch availability. The table also includes a 'Total: 3' indicator and a '1-3 of 3' pagination control.

Vulnerabilities	File Path	Exploit Status	Patch Availability	CVSS 3.0 Score	CVSS 2.0 Score
Vulnerabilities CVE-2020-17527 are fixed in 17 November...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2020-17527,CVE-2021-24122 are fix...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	7.5	5.0
Vulnerabilities CVE-2021-25329,CVE-2020-9484,CVE-20...	E:\CIS_SERVER\ManageEngine_Pri\DesktopCentral_Server	Not available	Not available	6.9	7.5

- The Software Vulnerabilities section enumerates vulnerabilities in the OS and third-party applications installed on the system.
- The Server Vulnerabilities section displays vulnerabilities in web servers, databases, or content management software installed on the system, if any.
- The Zero-day Vulnerabilities section displays the actively exploited and publicly disclosed vulnerabilities affecting the system.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

<p>identifies:</p> <p>for the at least one networked device, a first occurrence including at least one first occurrence packet, and</p> <p>for the at least one networked device; a second occurrence including at least one second occurrence packet;</p>	<p>ManageEngine <i>identifies, for the at least one networked device, a first occurrence including at least one first occurrence packet (e.g., Bad traffic), and for the at least one networked device; a second occurrence including at least one second occurrence packet (e.g., good traffic);</i></p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>How to prevent security misconfigurations?</p> <p>If vulnerabilities are the gateway to the network, it's the misconfigurations that attackers leverage to worm their way to the intended targets. Security misconfigurations are not hard to fix, but they are unavoidable in an enterprise operating at scale. Finding them is a needle in the haystack, as they can be located across any component in an organization's systems, such as its servers, operating systems, applications, and browsers. Lack of visibility and centralized means to remediate misconfigurations makes organizations fall victim to misconfiguration attacks.</p> <p>https://www.manageengine.com/vulnerability-management/misconfiguration/?mesearch</p>
--	---

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

As soon as it's up and running in your network, Vulnerability Manager Plus automatically discovers your Active Directory and workgroup assets. Scaling up? No problem. Since Vulnerability Manager Plus is constantly in sync with Active Directory, new assets will be brought under management as soon as they enter your network, leaving no opportunity for new threats to go unnoticed.

Leveraging endpoint agent technology, Vulnerability Manager Plus scans your laptops, desktops, servers, databases, workstations, and virtual machines across your entire global hybrid IT environment every 90 minutes, irrespective of whether they're within the corporate boundary or not.

You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ.

Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation.

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

DDoS prevention

We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing.

<https://www.manageengine.com/security.html?mesearch>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

	<p>Intrusion detection and prevention</p> <p>Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents.</p> <p>At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.</p> <p>At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.</p> <p>https://www.manageengine.com/security.html?meseach</p>
<p>determines:</p> <p>that the first occurrence including the at least one first occurrence packet directed to the at least one networked</p>	<p>ManageEngine <i>determines, that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable (e.g., Bad traffic); that the second occurrence including the at least one second occurrence packet directed to the at least one</i></p>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable;

that the second occurrence including the at least one second occurrence packet directed to the at least one networked device is not capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable, and

networked device is not capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable (e.g., good traffic), and;

Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):

How to prevent security misconfigurations?

If vulnerabilities are the gateway to the network, it's the misconfigurations that attackers leverage to worm their way to the intended targets. Security misconfigurations are not hard to fix, but they are unavoidable in an enterprise operating at scale. Finding them is a needle in the haystack, as they can be located across any component in an organization's systems, such as its servers, operating systems, applications, and browsers. Lack of visibility and centralized means to remediate misconfigurations makes organizations fall victim to misconfiguration attacks.

<https://www.manageengine.com/vulnerability-management/misconfiguration/?meseach>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

As soon as it's up and running in your network, Vulnerability Manager Plus automatically discovers your Active Directory and workgroup assets. Scaling up? No problem. Since Vulnerability Manager Plus is constantly in sync with Active Directory, new assets will be brought under management as soon as they enter your network, leaving no opportunity for new threats to go unnoticed.

Leveraging endpoint agent technology, Vulnerability Manager Plus scans your laptops, desktops, servers, databases, workstations, and virtual machines across your entire global hybrid IT environment every 90 minutes, irrespective of whether they're within the corporate boundary or not.

You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ.

Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation.

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

DDoS prevention

We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing.

<https://www.manageengine.com/security.html?mesearch>

EXHIBIT 12**U.S. Patent No 10,154,055 v. Zoho**

	<p>Intrusion detection and prevention</p> <p>Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents.</p> <p>At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.</p> <p>At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.</p> <p>https://www.manageengine.com/security.html?meseach</p>
causes a reporting of at least the first occurrence based on the determination that the first occurrence including the at least one first occurrence	<p>ManageEngine causes a reporting of at least the first occurrence based on the determination that the first occurrence including the at least one first occurrence packet is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable (e.g., mitigation capabilities to prevent disruptions caused by bad traffic).</p>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

<p>packet is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable.</p>	<p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>How to prevent security misconfigurations?</p> <hr/> <p>If vulnerabilities are the gateway to the network, it's the misconfigurations that attackers leverage to worm their way to the intended targets. Security misconfigurations are not hard to fix, but they are unavoidable in an enterprise operating at scale. Finding them is a needle in the haystack, as they can be located across any component in an organization's systems, such as its servers, operating systems, applications, and browsers. Lack of visibility and centralized means to remediate misconfigurations makes organizations fall victim to misconfiguration attacks.</p> <p>https://www.manageengine.com/vulnerability-management/misconfiguration/?meseach</p>
---	---

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

As soon as it's up and running in your network, Vulnerability Manager Plus automatically discovers your Active Directory and workgroup assets. Scaling up? No problem. Since Vulnerability Manager Plus is constantly in sync with Active Directory, new assets will be brought under management as soon as they enter your network, leaving no opportunity for new threats to go unnoticed.

Leveraging endpoint agent technology, Vulnerability Manager Plus scans your laptops, desktops, servers, databases, workstations, and virtual machines across your entire global hybrid IT environment every 90 minutes, irrespective of whether they're within the corporate boundary or not.

You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ.

Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation.

<https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html>

DDoS prevention

We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing.

<https://www.manageengine.com/security.html?mesearch>

EXHIBIT 12

U.S. Patent No 10,154,055 v. Zoho

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents.

At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

<https://www.manageengine.com/security.html?meseach>